EUCLIDEAN ALGORITHM

Theorem: Bezout's Theorem

Suppose $a, b \in \mathbb{Z}$ where $a, b \neq 0$. Let $d = \gcd\ (a, b)$ then d is the smallest possible integer that can be expressed as a linear combination of a and b $\quad (d = ax + by\ ,\ \ x, y \in \mathbb{Z})$

Theorem: Euclidean Algorithm

Let $a, b \in W$ such that:

a) If $a|b$, then $(a, b) = b$

b) If $b \nmid a$, then we do the following:

- $a = bq_1 + r_1 \qquad\qquad 0 \leq r_1 < b$

$\Rightarrow\ b = r_1 q_2 + r_2 \qquad\qquad 0 \leq r_2 < r_1$

$\Rightarrow\ r_1 = r_2 q_3 + r_3 \qquad\qquad 0 \leq r_3 < r_2$

.

.

.

$\Rightarrow\ r_{n-2} = r_{n-1} q_n + r_n \qquad\qquad 0 \leq r_n < r_{n-1}$

$\Rightarrow\ r_{n-1} = r_n\, q_{n-1} + 0 \qquad\qquad (a, b) = r_n$

Example 1: Find the gcd $(166, 196)$ using ***Euclidean Algorithm.***

Solution:

- $196 = 166\ (1) + 30$

$\Rightarrow\ \ 166 = 30\ (5) + 16$

$\Rightarrow\ \ 30 = 16\ (1) + 14$

$\Rightarrow\ \ 16 = 14\ (1) + 2$

$\Rightarrow\ \ 14 = 2\ (7) + 0$

Answer: The gcd $(166, 196) = 2$